Руководителю проекта
«Разработка комплекта документации по правовому обеспечению функционирования системы DLP»

Агеевой Елене Александровне

Участника проекта
«Разработка комплекта документации по правовому обеспечению функционирования системы DLP»

Махмадзиеев Али Олимович

Аналитическая записка

В современном мире все компании имеют собственную информационную инфраструктуру, включающую в себя автоматизированные системы, сети передачи данных, рабочие станции пользователей и т.д. Компания двигается в правильном направлении, когда задумывается о сохранности своих информационных активов и внедряет DLP-решение. Но если этому внедрению не сопутствует юридическое оформление, эффективность использования системы DLP снижается. Компания не сможет использовать данные DLP в суде против сотрудника, виновного в разглашении конфиденциальной информации (а может и пострадать от иска самого сотрудника за проведение мониторинга действий сотрудника без его согласия). В этой аналитической записке представляю законность использования системы DLP компанией для мониторинга действий работников, а также подробный план действий по реализации правомерного использования системы DLP в соответствии с законодательством РФ.

В соответствии с ТК РФ, 98-ФЗ(Федеральный закон от 01.04.2020 № 98-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам предупреждения и ликвидации чрезвычайных ситуаций"), 152-ФЗ (Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ) и пр., функционирование DLP в организации включает несколько аспектов, требующих юридического оформления. Еще один важный момент – большинство регламентов и положений требует подписи сотрудника, который либо выступает в качестве одной из сторон соглашения, либо подтверждает ознакомление с содержанием документа. Поэтому к работе над юридическим оформлением внедрения DLP необходимо привлекать HR-отдел(так как дело касается документов о не разглашении и тд. и т.п., любая

работа с сотрудниками касающаяся росписи каких либо документов должна проводится через HR-отдел) и, естественно, юристов. Некоторые компании, которые используют DLP систему прежде всего для учета рабочего времени работников, а не для контроля утечки конфиденциальной информации, предпочитают скрывать от сотрудников использование DLP систему

Прежде всего, надо понимать, что с юридической точки зрения конфиденциальными данными является не то, что компания хотела бы держать в секрете, а то, что формально закреплено в качестве информации ограниченного доступа. К информации ограниченного доступа относятся персональные данные, коммерческая, служебная, профессиональная тайна, сведения о сущности изобретения и пр. Поэтому первым шагом компания должна определить и документировать перечень информации ограниченного доступа, с которым сотрудники должны быть ознакомлены под роспись. Документы, которые понадобятся на данном этапе:

- Перечень информации ограниченного доступа.
- Перечень лиц, допущенных к обработке информации ограниченного доступа.
- Положения об обработке и защите информации ограниченного доступа (ПДн, КТ и пр.).
- Приказы о введении режима защиты информации (особенно КТ).

Теперь, когда мы выяснили, какую информацию будем защищать, и кто имеет к ней легитимный доступ, можно перейти непосредственно к вопросам ее возможного разглашения. В первую очередь, необходимо сформировать документы, в явном виде запрещающие разглашение сотрудниками информации ограниченного доступа, ставшей им известной в связи с исполнением трудовых обязанностей. Такой запрет должен быть прописан в документах двух типов: общие регламенты компании и документах, касающихся режима защиты информации.

Общие:

- Трудовой договор.
- Правила внутреннего трудового распорядка.
- Должностная инструкция работника.
- Положение о подразделении работника.
- Дополнительные соглашения с работником.

Режим защиты информации:

- Документы, содержащие положения и процедуры ИБ: общая политика ИБ, парольная защита, контроль доступа, защита от вредоносного ПО, допустимое использование ИС и сервисов (в т.ч. сеть Интернет и корпоративная почта), мониторинг и контроль, управление инцидентами, обучение и повышение осведомленности и пр.
- Инструкции пользователям информационных систем, сервисов и средств защиты информации.

Далее, как мы понимаем, запрет ничего не стоит, если не прописана ответственность за его нарушение. Лица, разгласившие информацию

ограниченного доступа, могут привлекаться к дисциплинарной, административной, гражданско-правовой, уголовной ответственности в порядке, установленном законодательством Российской Федерации. И, в частности, напомню, что разглашение охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, является основанием для увольнения сотрудника по инициативе работодателя (ТК РФ, статья 81, пункт 6в).

Следующим шагом необходимо составить локальные нормативные акты, определяющие правила обработки и защиты информации ограниченного доступа. Сотрудники должны быть ознакомлены с ними под роспись, и рекомендуется компаниям хранить копии журналов ознакомления.

Сотрудники должны знать (т.е. опять-таки расписаться в ознакомлении), что исполнение этих правил, как и использование корпоративных средств обработки информации, контролируется с использованием средств мониторинга.

Отдельно должны быть прописаны все правила, касающиеся личной информации сотрудников, ее хранения и передачи с использованием корпоративных ресурсов.

- Запрещено хранить личную информацию на корпоративных устройствах.
- Корпоративные каналы связи и средства обработки информации должны использоваться работниками исключительно для служебных (производственных) целей.
- Работникам запрещено хранить личную информацию на корпоративных ресурсах (рабочие станции и файловые хранилища) и передавать ее по корпоративным каналам связи (корпоративная электронная почта, сеть Интернет и другие).

Обязанности офицеров информационной безопасности также должны быть регламентированы и прописаны в положении о подразделении ИБ и должностных инструкциях его сотрудников. Как минимум, в список входят контроль соблюдения правил обработки и защиты информации ограниченного доступа и реагирование на инциденты информационной безопасности.

Система защиты информации должна соответствовать актуальным для компании угрозам, а также требованиям и рекомендациям регулирующих органов (Роскомнадзор, ФСБ России, ФСТЭК России). Что поможет офицерам информационной безопасности подтвердить это:

- Выписка из Модели угроз и Модели нарушителя.
- Выписка из ТЗ и ТП на систему защиты.
- Справка о DLP системе (функционал и сертификаты).
- Отчеты об аудитах и проверках ИБ, копии аттестатов соответствия.